# Analysis of the Country Reports

Nouwt, J.; de Vries, B.R.; Loermans, R.J.W.

*Published in:*
Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy

*Publication date:*
2005

# Chapter 13
# ANALYSIS OF THE COUNTRY REPORTS

**Sjaak Nouwt, Berend R. de Vries, Roel Loermans**[1]

## 13.1 Introduction

The focus of this book is on developments in the area of camera surveillance and workplace privacy. In the previous chapters, the contributors have analysed the case law and relevant legal provisions on these two issues in the specific country discussed.

In this chapter, we will combine key conclusions from the different country reports and draw some general conclusions. In doing so, we will start with an analysis of camera surveillance (13.2) and subsequently touch upon issues in the area of workplace privacy (13.3). Both sections are structured on the basis of the following three questions.

1. Does legislation matter in creating a certain level of privacy protection?
2. What role does case law play in this respect?
3. What future challenges can be expected?

After these sections, we will discuss differences between the use of the concept of reasonable expectation of privacy in the European, Canadian, and American contexts and we will conclude this chapter with some general conclusions and remarks (13.4).

## 13.2 Analysis of Camera Surveillance

### 13.2.1 **Does legislation matter?**

The concept of reasonable expectation of privacy originates from the United States where it was first used in the *Katz* case,[2] and is based on the Fourth Amendment to the US Constitution. The Canadians, who have a similar rule in their Constitution

[1] All authors are affiliated to Tilburg University, the Netherlands.
[2] *Katz* v. *United States*, 389 U.S. 347 (1967), PN 2004-68.

*S. Nouwt, et al. (Eds), Reasonable Expectations of Privacy?*

on unreasonable searches and seizures, followed their southern neighbours in the use of the reasonable expectation of privacy concept to some extent. In Europe, a similar concept has been used since 1992 by the European Court of Human Rights.[3] Therefore, both the section on case law and this section on the importance of legislation will start with a discussion of the United States, followed by Canada and the European countries.

#### 13.2.1.1 *The United States*

In his country report, Gellman argues that general United States surveillance law and policy for government and private actors lack clarity, coherence, consistency, compactness, and currency. Little of this general surveillance law applies directly to camera surveillance. Therefore, the law governing camera surveillance in the US is not very clear. However, the Fourth Amendment to the US Constitution, banning intrusive searches and seizures, constitutionally restricts government camera surveillance. Camera surveillance by government also has other statutory limitations. The Privacy Act of 1974 is applicable to personal information collected by federal agencies from a public place, as well as to personal information collected from a private place. The distinction between public and private places seems more relevant in the US surveillance case law than it is in the Privacy Act 1974. It is expected that, due to the evolvement of technology, the Privacy Act 1974, which established a set of fair information practices, will regulate videotaping by federal agencies in the near future.

Private parties are legally restricted in camera surveillance by several state laws that regulate video voyeurism (e.g., Granny Cams, Nanny Cams) and state camera surveillance and racial profiling. Many state laws protect four types of privacy invasions caused by camera surveillance: 1) unreasonable intrusion upon a person's privacy; 2) appropriation of a person's name or likeness; 3) unreasonable publicity given to a person's private life; and 4) publicity that unreasonably places a person in a false light before the public. These kinds of privacy invasions may be actionable at law through a private lawsuit (privacy torts). Continuous surveillance by private parties in public areas like streets, shopping malls, and stores seems to be violating the American privacy law, but this has not yet been made clear in case law.

Self-regulation also exists, for example, in the District of Colombia, where the City Council directed the Chief of Police of the Metropolitan Police Department to issue regulations on the use of surveillance cameras and technology. According to the Council, the Police Department may also enter into agreements with public entities and private parties.

---

[3] The first case was *Lüdi* v. *Switzerland*, Judgment of 15 June 1992, Publ. ECHR, Series A, No. 238, PN 2004-135.

### 13.2.1.2 *Canada*

In Canada there are privacy laws at both the federal and the provincial levels, applicable to different types of organisations, depending on the constitutional authority of the legislating government. A number of 'quasi-legal legislation' instruments (Guidelines issued by provincial Commissioners) are also of importance.

Since the 1960s and 1970s, six provinces have had statutes on tort liability for invading privacy. In British Columbia, violating the privacy of another wilfully and without claim of right constitutes a tort, actionable without proof of damage. Eavesdropping or surveillance may also violate privacy, whether or not accomplished by trespass.

From the *Kelowna* case,[4] we may conclude that the constitutionality of camera surveillance in Canadian cities by government bodies (in this case, the Royal Canadian Mounted Police) is still unsettled under the Charter. This case especially showed that different attitudes toward camera surveillance exist within the Canadian legal systems and courts.

Several people, from the Privacy Commissioner of Canada to former Supreme Court Justice Gerard La Forest, are of the opinion that the fundamental right to be protected against unreasonable search or seizure cannot be extinguished by simply informing citizens that their movements and activities may be monitored. The 'right to privacy' is far more important than the legal concept of reasonable expectation of privacy, according to the Privacy Commissioner. This is especially true in public places, where citizens have the privacy right to be 'lost in the crowd', without being systematically observed or monitored, particularly by the state. It can therefore be concluded that the reasonable expectation of privacy can be limited by informing the public, but more arguments are needed to limit the fundamental 'right to privacy'.

Despite, or thanks to, the general character of the Canadian law regulating camera surveillance, more precise standards for the use of video cameras by public agencies have been made by the provincial Privacy Commissioners. The existence of a reasonable expectation of privacy in Canada depends principally on the distinction between public and private places. Under statutory law, according to federal and provincial statutes, it is quite clear that information collected by camera surveillance is 'personal information', provided that the images make identification possible. However, under the federal Privacy Act, images need to be recorded to become 'personal information'.

### 13.2.1.3 *The European countries*

The legislation in the European countries on privacy and data protection is heavily influenced by legislation on the international and European levels. Therefore, both

[4] PN 2004-163.

the Council of Europe's *European Convention on Human Rights* and the various directives of the European Union will be discussed separately. Reducing the discussion to this European framework is not sufficient as the implementation of the EU directives differs between the countries and the European framework does not regulate all aspects of camera surveillance relevant in the context of privacy and data protection.

The legal framework for European Union Member States consists of international and national legal instruments.[5] At an international level, Article 8 of the European Convention on Human Rights (Council of Europe, 1950) protects the European citizens' privacy or 'private life'. Article 8 is elaborated in Council of Europe Convention No. 108/1981 for the protection of individuals with regard to automatic processing of personal data. Voices and images are considered personal data if they provide information on an individual by making the individual directly or indirectly identifiable. Individuals who are lawfully within a State's territory also have the right to free movement, protected in Article 2 of Additional Protocol No. 4 to the European Convention on Human Rights. Restrictions to these fundamental rights are only allowed when they are necessary in a democratic society and proportionate to the achievement of specific purposes. This means in general that citizens have freedom of movement and conduct without being subject to detailed monitoring.

At the meeting of the European Council in Brussels on 17 and 18 June 2004, the EU leaders reached an agreement on a new Constitutional Treaty for Europe. One of the key elements of the European Constitution is the Charter for Fundamental Rights. Article 7 of this Charter provides for the protection of private and family life, home and communications (privacy) and Article 8 for the protection of personal data (data protection). The European Constitution will enter into force when all Member States have ratified it, which implies popular consultations in some Member States.

The European Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC) is also applicable to the processing of sound and image data.[6] This is also the opinion of the Article 29 Data Protection Working Party, which drafted a working document (WP 89) to contribute to the uniform application of national measures for camera surveillance. In general, Directive 95/46/EC is applicable to the processing of personal data wholly or partly by automatic means. According to Article 2, paragraph a, of Directive 95/46/EC, personal data is any information relating to an

---

[5] Art. 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance,* 11750/02/EN, WP 89. Adopted on 11 February 2004.

[6] See *supra* n. 5, pp. 5-7; British Institute of International and Comparative Law, *The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data,* Report 16 May 2003. Available on the Internet <http://www.europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/biiclstudy-soundimage_en.pdf>. Last visited June 2004.

identified or identifiable natural person: 'an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. Image and sound data are also personal data even when a car number-plate or a PIN number is filmed, instead of an individual's face.[7] The type of media, techniques, and the communication tools used are irrelevant to determine whether image and sound data are to be considered as personal data.

Recitals 14-17 of Directive 95/46/EC explain that the Directive should also be applicable to techniques used to communicate these data if they relate to natural persons. The Directive is only applicable if the processing of sound and image data is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria. However, the Directive is not applicable when the processing of sound and image data is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not fall within the scope of Community law. If sound and image data are processed for purposes of journalism or of literary or artistic expression, Directive 95/46/EC is applicable in a restricted manner, according to Article 9.

According to Article 3, paragraph 2, Directive 95/46/EC does not apply to camera surveillance carried out by a natural person in the course of a purely personal or household activity. This is the case when a person installs camera surveillance for the distance control of what happens inside his home, like the prevention of theft. Natural persons should bear in mind, however, that, since the *Lindqvist* case,[8] uploading digital images of persons to a home page is considered 'automatic processing' and thus is within the scope of the data protection laws implementing the Directive.

According to Article 33 of Directive 95/46/EC, the European Commission will report, at regular intervals, in particular on the application of the Directive to the data processing of sound and image data relating to natural persons and will submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and of the state of progress in the information society. In 2003, a report was published by the British Institute of International and Comparative Law, which surveyed the legislation in the Member States transposing Directive 95/46 that relates to the processing of sound and image data.[9]

In some European countries, the installation and deployment of camera surveillance needs authorisation in advance by an administrative authority, sometimes represented by the data protection authority. Such specific regulations may differ

[7] See *supra* n. 5, p. 15.

[8] European Court of Justice, Case C-101/01, 6 November 2003, PN 2004-86.

[9] British Institute of International and Comparative Law, *The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data*. See n. 6.

depending of the public or private nature of the 'controller' of the equipment. In other countries, no specific laws for camera surveillance exist. In these countries data protection authorities have drafted opinions, guidelines, or codes of conduct to ensure appropriate application of the general data protection provisions. Such instruments drafted by national data protection authorities are available in the UK, in the Netherlands, and in Belgium. In Italy, the Video Surveillance Decalogue 2004 contains principles, duties, and obligations that must be complied with until a code of conduct on camera surveillance enters into force.[10]

The legislation in the *United Kingdom* that regulates CCTV is relatively recent. The privacy issue was highlighted by the Human Rights Act 1998, which implemented the European Convention on Human Rights in the UK, and in the revised Data Protection Act 1998, which implemented EU Directive 95/46/EC. Before 1998, CCTV was only regulated by erratic and inconsistent voluntary Codes of Practice that were hardly complied with. According to Edwards, in Chapter 5 of this book, the fact that there is still no specific legal regime to control CCTV has possibly resulted in the recognition of the UK as a CCTV surveillance hot spot. The only existing regulations for CCTV are to be found in the Data Protection Act 1998, the common law on privacy and breach of confidence, and the laws on criminal evidence which regulate the admissibility in court of information gathered by CCTV.

In addition, the Information Commissioner has recently issued both a specific CCTV Code of Practice and a Data Protection Code on Monitoring at Work, which refers expressly to camera surveillance and to the CCTV Code. The CCTV Code has recently been amended in light of the controversial case of *Durant* v. *FSA*,[11] in which the *English* Court of Appeal unexpectedly narrowed the wide interpretation of 'personal data'.[12] This case also had a serious impact on the regulation of camera surveillance in the UK, where the Data Protection Act 1998 and the Information Commissioner's CCTV Code of Practice 2000 are applicable. The *Durant* case has already resulted in a new Guidance Note on the applicability of the Data Protection Act 1998 to CCTV. The result of the new note is that the Data Protection Act is no longer applicable to 'basic CCTV systems', because they are not considered to collect 'personal data' relating to any person when they are not intended or able to 'focus' on any individual, although images of living, identifiable persons are captured. The rule of thumb is that the CCTV controller needs to decide whether the images that have been taken are aimed at learning about a particular person's activities. The personal private sphere is no longer essential for the applicability of data protection law, but the intentions and goals of the CCTV operator are.

The *Durant* case caused an unexpected change in the applicability of the law. According to Edwards, the case may well jeopardise the *legitimate expectations of*

[10] See *supra* n. 5, pp. 7-12.
[11] PN 2004-81.
[12] See Chapter 5 in this book.

*privacy* of UK citizens and employees. As a consequence, the expectations of privacy in the UK may also differ from that in the other EU Member States. That is why it was suggested that the *Durant* case should have been referred to the European Court of Justice.

In *the Netherlands*, the Personal Data Protection Act 2001 [*Wet bescherming persoonsgegevens*] is applicable to digital camera surveillance systems. The use of analogous camera surveillance systems does not fall within the scope of the Personal Data Protection Act, but, for example, within tort law. It may not be easy for citizens to determine whether the cameras that film them are digital or analogous, and therefore whether they fall within the scope of the Personal Data Protection Act 2001. However, the rules of thumb, drafted by the Dutch Data Protection Authority, and in particular the transparency principle, provide for the reasonable expectation to be monitored, therefore to expect privacy to a greater or lesser extent.

The Dutch government issued an instrument for camera surveillance in public places [*Handreiking cameratoezicht*]. This instrument, available on the Internet and on CD ROM, contains a check-list for stakeholders and consists of protocols, handbooks, and model regulations.

A specific law exists in the Netherlands which protects citizens against hidden camera surveillance. On 1 January 2004, the Penal Code was changed on the basis of the Hidden Camera Surveillance Act [*Wet heimelijk cameratoezicht*]. It is now a criminal offence to take pictures of places accessible to the public without informing the public. Furthermore, according to the Municipalities Act [*Gemeentewet*], city councils and mayors have the competence to allow the use of camera surveillance systems in public places for public purposes under certain conditions.

In *Belgium*, no specific law exists to protect privacy against camera surveillance. Article 8 ECHR protects the private life of Belgian citizens. However, the Commission for Human Rights concluded, in a Belgian case, that camera surveillance by monitoring, without recording pictures is identical to obtaining information on the spot, and therefore does not violate a person's private life. The Belgian Data Protection Act 1992 is applicable to camera surveillance, although the term 'camera' is absent in the Act. As a result, the status of data protection in Belgium with regard to camera surveillance is rather abstract and unclear.

According to De Hert and Loncke, the Belgian Data Protection Act is undisputedly applicable to camera surveillance. Although, furthermore, there is no legislative framework at the moment, but 'a great silence', important regulatory work has been done by the Belgian Privacy Commission and by the National Labour Council. In 1995, the Belgian Privacy Commission examined the applicability of the Belgian Data Protection Act to video recording. In 1998, the Commission published an opinion on a Bill concerning security through camera surveillance at football matches. In 1999, the Commission issued an opinion with regard to a draft Royal Decree about the installation and the functioning of surveillance cameras in football stadi-

ums. At the end of 1999, the Commission published, on its own initiative, an opinion on the processing of images through camera surveillance. In 2000, the Commission published an unsolicited opinion that dealt with the use of systems of camera surveillance in the entrance hall of an apartment building. In this opinion, the Commission examined the subject on the basis of compatibility with the Belgian Data Protection Act.

On 16 June 1998, the National Labour Council adopted Collective Labour Agreement No. 68. This Agreement deals with the protection of private life with respect to camera surveillance in the workplace. By signing this Collective Labour Agreement, employers accepted the prohibition of using secret methods to record visual images through camera surveillance.

In *Italy*, privacy related to camera surveillance is protected by human rights, like Article 8 ECHR, protecting the private life of the individual. Furthermore, Article 2 of the Italian Constitution protects human rights. Article 10 of the Italian Civil Code protects the individual's dignity or reputation against the use of visual images.

Directive 95/46/EC was implemented in Italy by the new Personal Data Protection Code, which entered into force on 1 January 2004. Based on Article 134 of this Code, the Italian Data Protection Authority issued the Generally Applicable Provision of 29 November 2000, which was renewed on 29 April 2004 (Decalogue 2004). The Decalogue 2004 contains principles, duties, and obligations that must be complied with until a code of conduct on camera surveillance enters into force. The Decalogue 2004 consists of general principles for camera surveillance: the lawfulness principle, the necessity principle, the proportionality principle, and the finality principle. The Decalogue 2004 also consists of a specific part with additional rules for camera surveillance activities, carried out in specific environments, like workplaces, hospitals, schools, places of worship, and cemeteries.

#### 13.2.1.4 *Conclusion*

The legal data protection framework may depend on several criteria. First, legal provisions that are applicable to camera surveillance may emanate from constitutional law or statutory law. Second, legal provisions may be drafted at a federal level or at state level. This is especially true for the US and Canada. Third, only general data protection law may be applicable or also specific data protection law. Fourth, the applicability of data protection law may depend on the use of digital techniques or analogous techniques of camera surveillance. Finally, the applicability of data protection law may depend on whether camera surveillance is deployed in public places or in private places.

There are great differences between the legal frameworks which are relevant for camera surveillance in the countries surveyed. In some countries, not every form of surveillance is regulated but a more important conclusion is that the reported coun-

tries also differ in the level of detail of the regulation. It is no surprise that the level of regulation in the United States is in general lower than it is in European countries but, even among those European countries, rather significant differences exist. In many countries, the lack of specific regulation seems to be compensated by the opinions, guidelines, and codes of conduct that are often drafted by the national data protection authorities, especially in Italy and the Netherlands. These documents can provide clear explanations of the legal framework for citizens and for 'controllers' of camera surveillance systems, and thus lead to a better understanding of what the reasonable expectations of privacy are. At this moment in time, it seems that self-regulatory instruments and opinions and guidelines given by data protection authorities are an adequate compensation for the lack of specific camera surveillance regulations. Whether they are adequate may in part be answered by the case law, which will be discussed in the next section.

### 13.2.2 **The importance of case law**

#### 13.2.2.1 *The United States*

Despite the many surveillance statutes and court decisions, law on camera surveillance in the United States is rare. Any judgments about standards for camera surveillance must largely be extrapolated from the general surveillance case law.

A distinction must be made between camera surveillance by government organisations and camera surveillance by private persons or organisations. Camera surveillance by government organisations is subject to different restrictions than camera surveillance by private parties.

Surveillance by government agents is regulated in different ways. The Fourth Amendment to the US Constitution limits unreasonable searches and seizures. It is important to note that not every use of camera surveillance is limited by the Fourth Amendment. First, it has to be established that the camera surveillance concerned actually constitutes a 'search' in the constitutional sense. In 1967, the US Supreme Court set a standard to determine when privacy falls under the protection of the Fourth Amendment in the renowned *Katz* case.[13] It stated that a person subjected to an intrusion of his or her privacy had to have had a reasonable expectation of privacy in order to be protected by the Fourth Amendment. According to the court, such a reasonable expectation exists if (1) a person actually has an expectation of privacy and (2) that expectation of privacy is also generally recognised as being legitimate. It should be noted, however, that this test does not say anything about the reasonableness of the search itself. So far, however, the main focus in US case law has been on the public private distinction when determining whether a person's privacy is protected by the Fourth Amendment. Gellman concludes that, in the light of new technologies, the importance of the private/public distinction might dimin-

[13] *Katz* v. *United States*, 389 US 347 (1967), PN 2004-68.

ish and will be replaced by the reasonable expectation of privacy concept, which provides a more adequate standard to decide cases where privacy intrusions by means of new technological devices are the core issue.

Nevertheless, the reasonable expectation of privacy concept as formulated in the *Katz* case has widely-recognised weaknesses. Technological developments can influence the privacy expectations of persons and can therefore also 'erode' the protection provided by the Fourth Amendment, since this Amendment only protects people who have a reasonable expectation of privacy. Case law shows us that the US Supreme Court struggles with the issue of the use of new technologies, an issue that will become more of a problem in the future, since surveillance technology is becoming cheaper and more widespread.

The *Knotts* case,[14] in which an electronic beeper had been attached to a vehicle to track its movements, is a good example of the Supreme Court's struggle. The Court stated that, because the movement had taken place in public thoroughfares, the person tracked had no reasonable expectation of privacy.

It took the Court nearly twenty years to acknowledge that an advancing state of technology could affect the privacy expectations of people. The *Kyllo* case[15] in itself did not offer much guidance because of the case-specific standards used by the Court. It did, however, leave the door open to future standards on the impact of technology on privacy expectations, since the court did recognise there might be constitutional limitations to surveillance from public places.

Privacy intrusions by private persons or organisations are regulated by several statutes and tort law. Much of this legislation appears to be an indirect result of new technology that enables people to surreptitiously film others.

In private litigation, tort law, the same main principles as in Fourth Amendment cases are applied: the private/public distinction and the more flexible reasonable expectation of privacy concept. Limitations to surveillance are recognised in tort law, even when it takes place entirely in a public place, and contains several precedents that find liability for invasion of privacy in such a situation.[16]

Gellman concludes that the reasonable expectation of privacy standard becomes more important when the more mechanistic public v. private place distinction is losing its value. Gellman expects that the reasonable expectation test will be used more in the future.

#### 13.2.2.2 *Canada*

The use of CCTV in public places or in a criminal investigation is not generally accepted in Canada. This impression is illustrated by numerous cases, both under

---

[14] *United States* v. *Knotts*, 460 US 276 (1983), PN 2004-77.

[15] *Kyllo* v. *United States*, 533 US 27 (2001), PN 2004-72.

[16] See: *Nader* v. *General Motors Corp.*, 255 N.E.2d 765 (NY 1970), PN 2004-128; *Galella* v. *Onassis*, 487 F.2d 986 (2d Cir. 1973), PN 2004-129.

constitutional law and under statutory law, in which the use of CCTV is bound by very strict limitations.

When camera surveillance is used by a government organisation, it falls under the Canadian Constitution. Even though Section 8 of the Canadian Charter of Rights and Freedoms resembles the Fourth Amendment of the US Constitution, its jurisprudence is not as well-developed as in the United States. There are only a few Canadian Supreme Court cases of relevance to the collection of personal information by means of camera surveillance.

By far the most influential camera surveillance constitutional case is *R.* v. *Wong.*[17] A number of important statements were made by the Court in this case. The Canadian Supreme Court was clearly influenced by the US Supreme Court when using the reasonable expectation of privacy test. However, the application of this test by the Canadian Supreme Court is somewhat different from the way the concept is used by its American counterpart.

To determine the privacy expectations of citizens, the Canadian court argued that the appropriate test was to consider whether the resulting loss of freedom of privacy from unauthorised surveillance is inconsistent with the standards of privacy that people might expect in a 'free and democratic society'. It also stated that an unreasonable search and seizure was not dependent on the technology used and that the fact that the accused were involved in illegal activities had no impact on their privacy expectations. In practice, this means that the privacy expectation of people is now principally determined by the location where the intrusion occurs. This can also be seen in the body of case law which offers a string of cases concerning the question of when locations are to be considered private and when public.

In contrast to the US case law, in Canada, no extensive body of case law exists that has developed further standards to determine when people have a reasonable expectation of privacy. As already mentioned by Gellman in his country report on US camera surveillance, the distinction between private and public locations as a standard for determining peoples' privacy expectations may, in the face of new technologies, become obsolete, since it offers inadequate protection from intrusions that are conducted in public places but are aimed at private places.

In civil cases, the use of CCTV in the workplace shows a different picture; even though the rights and interests of the employee are recognised by the courts, Bennett and Bayley signalled the difficulties employees face when relying on privacy claims, especially against powerful corporate interests.[18] Case law gives the impression that employees have a lower privacy expectation when they are at work and if their employer is not a government organisation.

---

[17] *R.* v. *Wong* (1990), 60 C.C.C. (3d) 460, [1990] 3 S.C.R. 36, 1 C.R. (4th), PN 2004-87.

[18] See *Le syndicat des travailleurs(euses) de Bridgestone-Firestone de Joliette (CSN)* v. *Me Gilles Trudeau et Bridgestone/Firestone Canada inc.*, C.A.M., 500-09-001456-953, 30 August 1999; *Richardson* v. *Davis Wire Industries Ltd.* (1997), 28 C.C.E.L. (2d) 101 (B.C.S.C.) at 114.

### 13.2.2.3 *Europe*

The concept of a reasonable expectation of privacy in European case law was introduced by the *Lüdi* v. *Switzerland* case,[19] a case in which the European Court stated that a person involved in criminal activities is entitled to a lesser expectation of privacy. According to De Hert,[20] it remains unclear why the Court did not check whether the intrusion by the government could be based on a national legal provision. It appears as if the Court did not want to check whether the government action in this case was in accordance with the protection provided by Article 8, paragraph 2 ECHR.

An application of the reasonable expectation of privacy concept as such can be found in the *Halford* v. *United Kingdom* case.[21] An employee's phone calls at her workplace were monitored by her employer. According to the Court, the employer's action was not in accordance with Article 8 ECHR, arguing that the employee concerned had a reasonable expectation of privacy when making the phone calls.

In *P.G. and J.H.* v. *United Kingdom*,[22] the court eventually moderated the use of the reasonable expectation of privacy concept, stating that the concept was merely one of the criteria that can be used to determine whether there has been a reasonable privacy intrusion.

The use of the reasonable expectation of privacy concept by the European Court has been subject to a great deal of criticism. The use of the concept might eventually lead to a lesser privacy protection, since some forms of privacy intrusions might fall outside of the protective reach of Article 8, paragraph 2 ECHR, if, in those cases, the Court finds the data subject was not entitled to any reasonable expectation of privacy and that therefore no 'interference' has occurred. In those cases a legal basis is no longer required for government actions.

As Edwards states in Chapter 5, the *United Kingdom* is one of the most closely watched societies in the world and CCTV seems to be broadly accepted. Case law does not show a different picture. In fact, the legal protection offered by data protection law against CCTV in the UK was seriously undermined in the *Durant* case.[23]

The *Durant* decision has some major consequences for the use of CCTV, the handling of the data derived from camera surveillance, and the privacy expectation of citizens.

---

[19] *Lüdi* v. *Switzerland*, Judgment of 15 June 1992, Publ. ECHR, Series A, No. 238, PN 2004-135.

[20] Fragments from Prof. De Hert's lecture at the privacy colloquium, 21 April 2004 at Tilburg University have been used here.

[21] *Halford* v. *The United Kingdom* (20605/92) [1997] ECHR 32 (25 June 1997), PN 2003-49.

[22] *P.G. and J.H.* v. *The United Kingdom* (44787/98) [2001] ECHR 546 (25 September 2001), PN 2004-199.

[23] *Durant* v. *FSA*, [2003] EWCA Civ 1746, PN 2004-81.

In this case, the Court narrowed the definition of 'personal data' and stated that data is only 'personal' if the information is 'biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or event that has no personal connotations'. The focus of the law's concern is no longer the degree of intrusion in a person's private sphere, but has now shifted to the intentions and goals of the CCTV operator when setting up and operating the cameras. If the intentions and goals are not to specifically track a (group of) person(s), the data gathered does not qualify as 'personal data'. The result of this ruling is that data gathered by a large number of surveillance cameras will no longer be protected by obligations imposed by data protection laws. It may be concluded that it has become easier to place and operate surveillance cameras, provided their goal is not to track a specific person or group of people. Especially in the case of more sophisticated systems, that are able to track and zoom in on people, not all the images collected will still be protected. There would be a lack of protection when images are recorded that do not qualify as personal data. Then, according to Edwards, the CCTV system seems to completely slip through the data protection net.

Another consequence of the *Durant* case is that persons whose images are thus casually collected, and whose images are thus not categorised as their 'personal data', will have no rights to access their data, nor, perhaps, rights to control how they are processed.

The degree to which people can have a reasonable expectation of privacy seems to have become less in the UK, especially with regard to data protection. Since, however, as Edwards states, the decision in the *Durant* case has not yet been brought to the European Court, the question of whether this decision is in accordance with the standards as set by Article 8 ECHR remains unsettled.

The fact that the UK lacks clear regulations on CCTV has forced the UK courts, when deciding cases involving CCTV images, to resort to standards that they would normally use for solving other legal issues. One example is the use of the concept of 'breaches of confidence' in a series of recent, well-known 'celebrity privacy cases' like *Douglas* v. *Hello!*[24] and *Campbell* v. *MGM.*[25] Even though this principle has been successfully invoked in these 'celebrity cases', the problem with CCTV and 'breaches of confidence' as the basis for invasion of privacy is that there is not necessarily a creation or exposure of confidence, when being filmed in public. The case of *Peck* v. *The United Kingdom*[26] dealt with this specific problem, ultimately resulting in financial compensation by the UK for lacking an effective remedy against the violation of privacy.

Another point of concern raised by Edwards is the fact that the UK courts, unlike their US counterparts, seem reluctant to dismiss evidence collected by means

[24] *Douglas* v. *Hello!* [2001] QB 967 (CA), PN 2004-166.

[25] *Campbell* v. *MGM* [2004] UKHL 22; [2002] EWCA 1373; [2003] QB 633 (CA), PN 2004-82.

[26] *Peck* v. *The United Kingdom* [2003] EMLR 15, PN 2004-84.

of an illegal use of CCTV. Rules on the admissibility of evidence are an effective tool when promoting good practice in the administration of CCTV schemes, but the UK courts seem to accept, almost automatically, video and still images collected by CCTV. This reluctance to dismiss evidence resulted in compensation by the European Court in *Perry* v. *The United Kingdom* because it constituted a breach of Article 8 ECHR.[27]

As stated by Edwards in her country report, the lack of UK regulation on the use of camera surveillance has had a major influence on the use of cameras. Case law has only done a mediocre job at best to fill in the legislative gap and several decisions by the European Court have been the result. At this moment, the question is whether the principles formulated in the *Durant* case are in accordance with the ECHR.

The case law, referred to in the country report from *the Netherlands*, concerns camera surveillance in public places and private places. Camera surveillance in public places can be applied for observations by the police, for the prevention of public order offences within municipal boundaries, or to some extent by private parties, for example, in co-operation with the police. Camera surveillance in private places can be applied to monitor employees in the workplace, and in non-contractual relationships, for example, for security, property protection, or other reasons. In Dutch case law, the lawfulness of camera surveillance has been tested in several contexts, especially in the area of criminal law and in employment disputes.

In most of the case law about camera surveillance in public places, the main question concerns the legitimacy of police observations. In answering this question, the criterion of 'more than a small degree of interference with privacy' plays a key role. The Dutch case law is rather casuistic, but it does give some insight into the legitimacy of camera surveillance in public places. In criminal case law, the seriousness of the criminal offence, the frequency, and the effects of the offence for other citizens seem to be relevant in determining the level of privacy for suspects of criminal activities. An example is the permanent use of surveillance cameras in the Rotterdam district of 'Saftlevenkwartier', which was judged to be lawful because of the nuisance that the drug selling and trafficking caused in that neighbourhood. Similarly, it was decided that repeatedly committed sexual offences in a neighbourhood were there are many children can justify observation by cameras for a longer period. However, other circumstances are also relevant to determine whether a citizen suffers 'more than a small degree of interference with privacy': the duration of the observation, the intensity, the location, the purpose, and the way in which the observation takes place.

In a recent case, the Dutch Supreme Court concluded that the evidence obtained by permanently installed cameras in the city centre of Rotterdam could be used against a graffiti sprayer. The Supreme Court said that the cameras were covering

[27] *Perry* v. *The United Kingdom,* ECHR, Application No 63737/00, 2003, PN 2004-85.

areas in a public place, where the suspect had no reasonable expectation of privacy. The Supreme Court concluded that the interference with the right to privacy of the suspect during the time he and his accessories had been observed was too limited to be a real interference, because the purpose of the observation was to prevent disorder in public places. Moreover, the surveillance had been conducted by means of more than one fixed and movable camera in accordance with a legitimate procedure. According to the Supreme Court, such an observation is never an inadmissible interference with regard to Article 8, paragraph 2 ECHR. With this decision, the Supreme Court followed the *Lüdi* decision of the European Court of Human Rights (ECHR) and introduced a third situation, namely, one that does not constitute a breach of privacy at all.

In private places in the workplace, a suspected employee may lawfully be subjected to camera surveillance to a greater extent than other employees. The concept of a reasonable expectation of privacy is used to some extent, but it is primarily used to legitimise certain privacy-invasive measures.

A famous Dutch case is the *KOMA* case,[28] dating from the 1980s. According to this case, an employer is allowed to install cameras when he has a legitimate interest. Legitimate interests include, for example, the protection of installations against theft or destruction by third parties, or the continuous, visualised, and simultaneous protection at different places of highly mechanical and complicated technical production processes. Later, several other judgments about the use of cameras at the workplace were published. Most cases concerned the use of cameras against theft.

In non-contractual private relationships, privacy is to be expected in the rest room of a casino or in a fitting room of a store. Retailers who use camera surveillance must always inform their customers and their personnel. Camera surveillance to protect a house is allowed as long as the camera does not focus on the street or films inside another house. It should also be made clear to visitors that camera surveillance is being used.

In *Belgium* there is no culture of bringing privacy issues to court. This is due to the fact that there is a great dislike of creating negative publicity, which unfortunately has also had the negative consequence that judges have not had the opportunity to express their opinions on the subject very frequently.

The Belgian case law on the subject of CCTV is not characterised by coherence, consistency, or even quality. In the Belgian country report, a series of cases is mentioned in which the courts proved to be either unfamiliar with data protection or the data protection authority's work or were downright reluctant to apply their standards.

There is an unwillingness to apply some of the 'hard' procedural data protection norms. Courts seem to favour using other standards that provide them with more freedom. The fact that softer standards are being applied in Belgian case law has

[28] PN 2003-66, PN 2003-67.

had the unfortunate consequence that data enjoy less protection than they would have had if the harder data protection standards had been used. Some examples of softer standards are the use of the concept of the 'duty to respect' and the balancing of interests in the context of Article 8 ECHR. Equally important is the fact that the evidential regime in Belgium is free (meaning that even evidence gathered by means of an illegal use of CCTV could still be accepted in legal procedures). However, there are also examples of a more correct use of both the 'hard' and 'soft' standards by the courts.

In the end, the case law on this issue in Belgium does not show any tendency towards limiting the use of CCTV, despite the efforts made by the Belgian Privacy Commission, whose advice is not reflected in the case law, either.

According to Balboni in his country report, the case law in *Italy* is consistent. There is a high awareness of data and privacy protection, which can be seen in the joint efforts by the courts and the Garante, the Italian data protection authority, in enforcing data protection principles and duties. However, in Italy, case law is secondary to laws and guidelines as far as the creation of standards is concerned, since the legal provisions in Italy are quite extensive. Examples are the new Personal Data Protection Code 2004 and the Decalogue 2004, containing principles and duties that have to be obeyed, such as the four general principles which must be complied with when processing personal data by means of camera surveillance: the lawfulness principle, the necessity or data minimisation principle, the principle of proportionality, and the finality principle.

#### 13.2.2.4 *Conclusion*

The country reports teach us that the concept of a reasonable expectation of privacy is mainly used in the United States and Canada. The application of the concept in these countries is very different. The ECHR has also more or less introduced the concept into European human rights case law, but has not adopted the concept as the core principle in privacy protection. The reason for the ECHR's hesitation might be the fact that applying the concept might ultimately result in a diminished privacy protection, since the definition of privacy is linked to public expectations concerning the concept.

On a national level, courts in Europe do not use the concept as such and quite often rely on solutions offered by other legal provisions, such as concepts used in civil law or labour law. In some countries, e.g., the Netherlands, this has led to a pragmatic approach when dealing with privacy issues, which has its advantages (flexibility) and disadvantages (legal insecurity).

The lack of specific legislation on camera surveillance has led to different results in different countries. The United Kingdom has become a surveillance hot spot, an example that has not been followed in other countries, where case law has played an important role in restricting the use of camera surveillance. Even though

there is a lack of legislation on the use of CCTV, courts in European countries will have to use the legal backdrop provided in Article 8 ECHR and the case law on the provisions in this article.

### 13.2.3 **Future challenges**

It seems to us that the fact that only general data protection law exists, and no specific laws, makes no difference for the level of protection against camera surveillance. At the privacy colloquium we organised on 21 April 2004 concerning 'Reasonable Expectations of Privacy', Koops pointed at the growing possibilities of surveillance technologies, which can have consequences for the reasonable expectation of privacy that citizens can have. Camera phones are becoming commonly used mobile phones. Webcameras are within reach of nearly everyone who can afford a computer. Satellite pictures, thermal images, and face recognition are also more and more commonly used technologies. Not only new inventions, but also existing technologies that become available for a large user group may lead to greater risks of interference with the right to privacy.

Gellman describes the possibility suggested by the US Supreme Court in the *Dow Chemical* case[29] of a limitation on the use of satellite technology: 'It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be unconstitutionally proscribed absent a warrant'. In this case, however, the Court concluded that the aerial photographs of the industrial plant complex from navigable airspace did not reveal intimate details, and that technology was only used to enhance human vision somewhat.

On the one hand, it looks as if the broad availability of surveillance technologies for the public determines the margin of privacy protection, as is illustrated by the *Kyllo* case.[30] At the same time, the expectations seem less reasonable when surveillance technologies are only used to slightly enhance human vision.

Gellman also points to technologies that erode the important difference between public and private areas which can be monitored by camera surveillance. In the *Kyllo* case, the thermal surveillance of a home took place from a public place. Upskirt photography, possible nowadays by means of camera phones, also accentuates the inadequacy of the difference between public and private places. It seems that, to a greater extent, privacy can be invaded by surveillance from public places.

Bennett and Bayley conclude in their report that individuals now have easy access to the tools of private investigators. These products can be used, for example, to watch children's browsing behaviour, monitoring in child care centres (Nanny Cams)

---

[29] *Dow Chemical Company* v. *United States*. 476 U.S. 227 (1986), PN 2004-125.
[30] PN 2004-72.

and people in nursing homes (Granny Cams), enhancing home security, keeping an eye on contractors, baby-sitters, etc. Product manufacturers sometimes lure their customers by pointing at other possible applications of webcams, often without realising that monitoring baby-sitters, contractors, or employees without their knowledge or consent may be illegal.

Balboni points at the cheap and easy method of recording images by camera surveillance. Miniaturisation has led to an improvement in controlling equipment security, quality, productivity, and the regularity of labour performance. CCTV is increasingly used for crowd management in the transportation sector, like in subways and the nearby areas, but also within public buildings, and in recreational areas. Companies are even given a reduction in insurance premiums when they have camera surveillance systems installed. It can be assumed that no privacy instructions are delivered with the equipment.

Not only technological, but also legal challenges exist. With reference to the ECJ case of *Lindqvist*,[31] Edwards welcomes the result that data protection law covers the use of web cameras. Webcams are cheap, and therefore widely used. Outdoor webcams are a growing source of surveillance, often overlooked and unregulated.

However, state and private interests to control crime and anti-social behaviour operate the most ubiquitous cameras in the UK. Such camera surveillance for national security and crime prevention purposes is generally exempted from data protection law.

## 13.3 Analysis of Workplace Privacy

### 13.3.1 **Does legislation matter?**

#### 13.3.1.1 *The United States*

In the US, workplace privacy has become a social issue in the last few decades because of the fact that, in a growing number of cases, employers have been held liable for their employees' activities and, for this reason, employers started monitoring their employees' actions on a larger scale. New technologies made monitoring cheaper and more pervasive. These practices became subject to legislative and judicial review.

Phillips points out some interesting patterns between privacy and other social values. First, it often seems unclear whether an individual is protected by the right to privacy, or an organisation of individuals, or some special places: private or public. There is a risk that, when focusing on private places, courts may sooner allow monitoring in public places. Second, expectations of privacy may be place-

[31] PN 2004-86.

related. A workplace is a private place of the owner: the employer. Nevertheless, employees who use these private places are offered some protection. How much protection an employee can expect also depends on the hierarchy within the company: managers seem to have more privacy than employees on the shop floor, because the managers can close their office doors. Third, regulating workplace privacy is often focused on physical artifacts or techniques as the primary object of regulation, instead of the social relationship between the employer and his employees. Because the federal Electronic Communications Privacy Act focuses on aural monitoring, courts were free to ignore video monitoring. Workplace privacy regulations may thus be too 'technologically dependable'. It seems better to focus workplace privacy on the social relationship. Finally, Phillips points at a reduction of the expectation of workplace privacy by the use of consent from employees. Because employees reduce their reasonable expectations of workplace privacy by giving consent to an employer's search and monitoring policies, employers nowadays demand such consent as a standard business procedure. As a result, consent to search and monitor is becoming implicitly acknowledged in the employment relationship. Adopting such a standard business procedure into regulation can diminish privacy expectations.

We may conclude that Phillips illustrates that workplace privacy regulations should focus on the social employment relationship, rather than on specific places, or objects, or technologies. From this point of view, it is interesting to point at the European ideas for a special Directive for the protection of employee data (see section 13.3.3: Future challenges). At this point, we will first analyse the workplace privacy regulations from the country reports.

#### 13.3.1.2 *Europe*

In Chapter 5, Edwards describes the data protection framework in the *United Kingdom* for CCTV in the workplace. European data protection law and European human rights law have been implemented in the UK and require a balance to be drawn between the employer's legitimate interests and the employee's right to privacy and data protection. The general CCTV Code of Practice does not explicitly apply to the workplace, but only to public places. However, the Information Commissioner introduced the Employment Practices Data Protection Code in 2003, which explicitly deals with monitoring at work. However, this Code still has only an advisory status. It suggests 'impact assessment' as the best way to approach workplace monitoring. The Employment Code of Practice specifically suggests that the CCTV Code may be useful by analogy to employers. Video and audio monitoring should be aimed at areas of particular risk, and confined to areas where expectations of privacy are low. The vague platitudes of the Employment Monitoring Code might give rise to blanket CCTV monitoring in the workplace. However, such CCTV monitoring can be challenged as an infringement of Article 8 ECHR or of the common law rights of privacy.

In *the Netherlands*, the legal framework consists of constitutional protection, general data protection law, and employment law. Article 10 of the Dutch Constitution, guaranteeing respect for privacy, provides constitutional protection. Article 8 ECHR is also applicable to protect privacy, including workplace privacy, in the Netherlands. The Dutch Civil Code contains a typical labour law provision. Article 7:611 requires employers and employees to act in good faith. This concept of 'good employership' gives indirect horizontal effect to the right of privacy for employees.

The Personal Data Protection Act also applies to employer-employee relationships. The Works Council Act [*Wet op de ondernemingsraden*] is applicable to the processing of personal data by employers. The employer who intends to implement, alter, or withdraw rules for the processing of employee data needs the works' council's consent.

Related to the processing of employees' medical data, the Sickness (Absence) Reduction Act [*Wet terugdringing ziekteverzuim*] is applicable. To be able to fulfil their obligation to continue payment for sick employees, employers need to process their employees' medical data to a certain extent. Another applicable law concerning employees' medical data is the Medical Examinations Act [*Wet op de medische keuringen*]. This statute only allows medical examinations of employees or applicants when this is necessary for the job.

In 2000 the Dutch Data Protection Authority [*College bescherming persoonsgegevens: CBP*] published a study, entitled Working Well in Networks [*Goed werken in netwerken*], about monitoring, the use of the Internet and e-mail in the workplace. As a result, the Dutch Data Protection Authority formulated rules of thumb for employers who check their employees' use of the Internet and e-mail. The Dutch Data Protection Authority also developed a legal framework for the use of e-mail and the Internet in the workplace. Employers can use this framework as an instrument to translate the rules of thumb to their own company policy. The Confederation of Netherlands Industry and Employers [*VNO-NCW*] and the largest trade union federation in the Netherlands, FNV Bondgenoten, also developed a model code of conduct and a model protocol for employees and works' councils as an instrument to regulate the use of e-mail and the Internet in the workplace.

Important for the protection of workers' privacy in *Belgium* were the *Niemietz* case and the introduction of several privacy-related statutes. One of these statutes is the Data Protection Act [*Wet verwerking persoonsgegevens*] of 8 December 1992, which, for example, restricted the employers in screening workers, clients, or economic partners. Another relevant statute is the Act of 30 June 1994 for the protection of privacy related to monitoring and interception of communications. This statute introduced a general prohibition into the Belgian Criminal Code (Article 314*bis*), leaving employers no possibility to listen to the telephone conversations of their employees without their consent. The Act of 21 March 1991 (the 'Belgacom Act') prohibited the examination of communications, including e-mails and fax messages, without the consent of all persons directly or indirectly involved (Article 109*ter*).

Articles 314*bis* and 109*ter* are both based on the principle that the content of data may be examined only with the consent of the employee and the other parties involved. This principle has led to several uncertainties about the applicability of the articles. Because these articles only protect communication in transmission, it was not clear, for example, whether a *sent* e-mail, which has not yet been read by the employee, was protected by either one of them. It was not clear either whether visiting a web site should be considered a communication.

Workplace privacy in Belgium is also protected in specific privacy regulations. With reference to the case law of the European Court of Human Rights, concluding that the protection of privacy includes activities of a professional or business nature, the Belgian Privacy Commission issued an opinion in 2000 regarding monitoring by the employer of the use of computer systems in the workplace. Furthermore, on 26 April 2002, the Belgian National Labour Council signed a national collective agreement on the protection of the privacy of employees concerning the monitoring of electronic on-line communications data.

In *Germany*, there is a high density of data protection legislation. In 1977, the Federal Data Protection Act [*Bundesdatenschutzgesetz, BDSG*] came into effect. In 2001, the *BDSG* was amended to implement the EU Data Protection Directive into German law. At state level, every German state has its own Data Protection Act [*Landesdatenschutzgesetz, LDSG*]. Several German information and telecommunication statutes are supplements to the *BDSG*: the Telecommunications Act [*Telekommunikationsgesetz, TKG*], the Telecommunications Data Protection Ordinance [*Telekommunikations-Datenschutzverordnung, TDSV*], and the Teleservices Data Protection Act [*Gesetz über den Datenschutz bei Telediendsten, TDDSG*].

Although a special law for workplace privacy does not exist in Germany, there is other legislation that influences the protection of employees' data. The Works Council Constitutional Act [*Betriebsverfassungsgesetz, BetrVG*] ensures the independent representation of the interests of employees. The most important provision in this Act is Article 87, which grants the works' council the right of co-determination if an employer wants to use technical facilities intended for monitoring the conduct and efficiency of the employees at work. Furthermore, Article 611 of the German Civil Code [*Bürgerliches Gesetzbuch, BGB*] and the principle of utmost good faith in article 242 of the Civil Code contain a fiduciary duty for the employer. Article 201 of the Penal Code [*Strafgesetzbuch, StGB*] protects employees against recording non-publicly spoken words and against eavesdropping.

It is possible in Germany to make special agreements for the processing of employees' data. Such agreement may be collective labour agreements or consent forms by which employees agree to restrictions of their constitutional right of personal freedom.

The current German cabinet has plans to present a bill regulating privacy in the workplace within the legislative period of 2003-2008. The European Commission is also working on expanding the legal framework for data protection (see also

section 13.3.3: Future challenges). It seems that Germany strongly supports the need for specific EU legislation on employees' privacy.

*Hungary* is one of the first countries in the Central and Eastern European region that treats data protection not as a separate subject but as an element of information rights. The Hungarian model of information rights consists mainly of personal data protection and the protection of data of public interest. Personal data protection is based on the fundamental right of self-determination, which is derived from the right to human dignity as a general personality right. Public interest data are based on the principle of openness. Following the Canadian example, both information rights are elaborated in the combined Data Protection and Freedom of Information Act (DP&FOIA). It entered into force in de mid-1990s. At that time, also sector-specific laws on the handling of information, like the Direct Marketing Act, the Identification Act, and the Medical Data Act passed through Parliament. The Criminal Code and the Civil Code further protect personal data.

The Hungarian privacy legislation is based on EU Directive 95/46/EC. As a result, Hungary was one of the first countries on the white list of third countries with an adequate level of protection. Hungary has been a member of the EU since 1 May 2004. Hungarian data protection legislation is sometimes stricter than EU Directive 95/46/EC and the Council of Europe regulations (Convention 108, Recommendations), especially for the transfer of personal data to third countries.

The Hungarian law on data protection consists of a general statute, which contains the most important data protection principles. Mandatory rules associated with various types of data and different data controllers can be found in sector-specific statutes. However, there is no sector-specific law to protect employees' personal data. Neither the Hungarian Labour Code nor any other sector-specific law protects the privacy of employees. The Labour Code only protects the personal data of newly recruited employees. This means that the general rules for data protection must be applied to employees' data. However, the Labour Code does allow the employer to check certain employees' data. Part of the data collected through a satellite surveillance system to keep track of the time spent at work can be processed legally. The employer is not allowed to use these data to keep track of the route that an employee has followed.

In *Italy*, the new Personal Data Protection Code [*Codice privacy* or *Testo unico sulla privacy*], which became effective on 1 January 2004, protects employees' personal data. The Personal Data Protection Code consists of general data protection principles. According to the Personal Data Protection Code, the Italian Data Protection Authority [*Garante*] must encourage the adoption of a code of conduct concerning the processing of personal data by public and private entities for the management of employer-employee relationships.

Employees' data are also protected in specific legislation: the Workers' Statute. It limits the possibilities for employers to collect personal data of applicants,

to monitor teleworking and on-line activities, and to use CCTV in the workplace.

In none of the European countries reported on does specific workplace privacy law exist at a national level.[32] However, the national data protection authorities have drafted codes of conduct, rules of thumb, and legal frameworks as an answer to the many questions they received from employers and employees. The absence of specific workplace regulations may be the cause of uncertainties and obscurities concerning workplace privacy issues, like the monitoring of employees' e-mail and their Internet use. Guidance by the national data protection authorities and employers' and employees' organisations, by developing model regulations, seems very useful.

Collective labour agreements regulating workplace privacy are known in Belgium and Germany. The German Cabinet has plans to draft a workplace privacy bill. In Italy, several provisions that protect employees' privacy are laid down in the Workers' Statute.

From the fact that only general data protection statutes and other general constitutional and labour laws regulate workplace privacy, we conclude that such a legal framework is too general to provide sufficient and useful conditions to balance workplace privacy and the legitimate interests of employers. To fill this gap, national data protection authorities, labour councils, and courts play an important role at the moment. Perhaps some changes will be forthcoming at the European level.

### 13.3.2 **The importance of case law**

Because of the great variety of legal vehicles in the *United States*, and hence the moral and ethical doctrines applied in each case, resulting from differences in jurisdiction and situations, it is very difficult, if not impossible, according to Phillips, to lay out a cogent and complete set of cases describing a regime of privacy protection within the US workplace.

As mentioned in Phillips' country report, public employees can start a case on constitutional grounds whereas employees of private companies are limited to tort and statutory law. Public employees can base their case on the Fourth Amendment. The *Katz* test has to be applied to determine the reasonableness of the employees' privacy expectations in light of the totality of the circumstances surrounding the particular incident. According to Phillips, specific case studies show that courts have held that the reasonableness of privacy expectations varies considerably with the physical locale and cultural norms surrounding the activity, and that the work-

[32] Only in Finland does a specific workplace privacy statute exist: the Act of May 2001 on the protection of privacy in working life (477/2001). See *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data* (DG Employment and Social Affairs). On the Internet <http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf>. Last visited: July 2004.

place reasonably entails very low expectations. Moreover, other public interests may override privacy expectations, making an intrusive search reasonable.

In tort law, in general, the same *Katz* test applies to the adjudication of a tort as applies to the constitutionality of warrantless searches. Phillips states that 'reasonableness' takes on special properties in the workplace and explains how it differs from the conventional application of the reasonable expectation concept. First, notice and consent may each destroy a reasonable expectation. Secondly, there must be a solitude or seclusion to be intruded upon, which means that an observation in public places does not constitute an invasion. Finally, the offensiveness of the intrusion may be weighed against other interests, such as business purposes or public safety, in ascertaining reasonableness.

Case law does show that the privacy expectations of employees both in public and private service are fundamentally lower than outside the workplace.

The use of the reasonable expectation of privacy concept rather than having a strict regulation on CCTV has not helped to increase the privacy of employees. The case law as presented in the country report shows a decreasing level of legitimate privacy expectations. This development is also fuelled by the 'at-will' employment doctrine in the US, meaning that no employer can be required to hire or retain an employee, and that no employee can be required to accept a job. Therefore, employees are in a more vulnerable position in relation to their employers.

*The Netherlands* lacks specific workplace privacy legislation. This is why case law plays an important role in the protection of the privacy interests of employees. Currently, the issue that is generating the larger part of the case law concerns the workplace monitoring of e-mail and Internet use.

It is not easy to distinguish any general principles that are used by the courts in protecting privacy in the numerous cases available. The body of Dutch case law is mainly characterised by a very pragmatic approach by the courts when addressing workplace privacy-related issues. One of the reasons for this approach is that, instead of basing their decisions on the Dutch Personal Data Protection Act, judges seem to prefer using general labour legislation that contains open norms and allows judges a free hand in balancing the interests of the employers against the interests of the employees. In many of the cases, the courts use the rather vague standard of 'good employership' as formulated in the Dutch Civil Code, when judging privacy intrusion by employers.

This clearly has some advantages; it allows courts to refrain from 'mechanically' applying data protection rules and provides them with a higher degree of flexibility. Ultimately, this should lead to a better quality of court decisions, because all the circumstances of the case can be taken into account.

There is also a major downside to this flexibility. Not having many general principles that can be applied leads to a high level of uncertainty amongst both employers and employees as far as the outcome of cases is concerned.

In *Belgium*, workplace privacy issues began to be taken to court after the *Niemietz* case.[33] European case law, especially with regard to Article 8 ECHR (private life), has played an important role in the protection of workplace privacy. After the judgment of the Court of Cassation, the Belgian Supreme Court of 27 February 2001, it was accepted that the provisions of Article 8 ECHR have horizontal effect.

Belgian case law did not offer legal security or solutions to privacy problems. Often no reference is made to the legal constitutional framework or to the criteria of the second paragraph of Article 8 ECHR, principles such as 'the duty to respect each other' are applied. In the case law that is available in Belgium, the reasons and outcomes vary strongly and the focus is often not primarily on the legality of the employer's control, but on the legality of the subsequent dismissal. There appears to be a tendency towards settling the matter out of court in order to avoid negative publicity.

Despite being rather densely regulated, *Germany* has no specific law to regulate workplace privacy. The result is that courts have to use other regulations and laws to deal with workplace privacy issues.

The German Constitutional Court[34] stated that data privacy is a constitutional civil right. The Court derived this right from the constitutional basic principle of free development of personality. More constitutional rights to protect the privacy of employees were deduced from this principle: private sphere and private protection, the right to verbal communication, the right to one's own image, the right to informational self-determination. Other basic constitutional principles that are used to regulate workplace privacy are the right to human dignity and the right to secrecy of telecommunications. Employees are allowed to waive constitutional rights connected to privacy, as long as the agreement does not violate the basic principle of human dignity.

Privacy in the application stage shows the problem of an applicant who might feel 'forced' to answer questions in order to be hired. The German Labour Court, aiming to protect applicants, found the basic rule stating that an employer is only allowed to ask questions that can actually be used in the selection of applicants and in which the employer has a qualified, legitimate, and meritorious protection interest.[35]

Telephone surveillance by the employer has to meet the conditions of a person's constitutional right to his spoken word and is therefore not allowed very frequently. This holds true for both private and business calls but there are some minor exceptions to this rule. On e-mail and Internet monitoring, no Constitutional Court decision has yet been delivered.

The fact that there are no specific regulations concerning workplace privacy in Germany does not at all mean that protection is inadequate. Case law has played a

[33] *Niemietz* v. *Germany* (13710/88) [1992] ECHR 80 (16 December 1992), PN 2004-200.
[34] BVerfGE 65, S.1.; (population census judgment), PN 2004-189.
[35] BAG, *NZA* 1986, p. 739.

major role in the protection of employees against privacy intrusions in more than one area. However, since the availability of new technologies also raises new privacy concerns, it is unclear what privacy expectations an employee is entitled to. The absence of specific regulation is a drawback for the principle of legal security, which is illustrated by the current legal hiatuses surrounding the surveillance of Internet and e-mail use by employers, since no Constitutional Court decisions on these issues have been available so far and lower courts operate completely independently from each other and do not have to abide by each other's precedents.

*Hungary* does not have sector-specific legislation on workplace privacy. The result is that judges have to resort to other, more general statutes and forms of regulation.

Hungarian courts seem reluctant to apply the Data Protection Act. Even if they do choose to base a decision on provisions in this statute, they often draw contradictory conclusions. The courts prefer to use the provisions in the Civil Code which also protect the rights of persons but the use of which will lead to different results, because of a different underlying ratio.

The absence of specific data protection laws in employment relations has also contributed to the situation in which the power balance between employers and employees, who are already reluctant to start any legal proceedings, due to their economically vulnerable position, might tip in favour of the employers.

Another point worth mentioning is that people whose privacy has been intruded upon will prefer to file a complaint with the Data Protection Commissioner rather than to start a procedure at the regular courts, which are considered to be slow and expensive and, most importantly, deliver unpredictable judgments. The Commissioner uses general rules of data protection, a set of normative directives on the application of data protection law, and is already responsible for a vast body of case law, also on a large number of workplace privacy-related issues. One important legal principle used by the Commissioner is the finality principle, meaning that employers are only entitled to gather the information they actually need, for one or more legitimate purposes, in their function as employers. The concept of a reasonable expectation of privacy as such is not one of the fundamental concepts used by either the Hungarian courts or the Data Protection Commissioner. Instead, they base their legal arguments on general and sectoral laws or, in the case of the Commissioner, on his own body of case law.

The Hungarian legal system, despite not having sector-specific workplace privacy legislation, seems highly adequate to protect the privacy interests of employees. However, especially in the light of Hungary being a 'new' European democracy and the introduction of the capitalist system, the position of employees has become more vulnerable to the power of employers. The Hungarian legal system insufficiently protects those employees who, because of their vulnerable situation, are hesitant to come forward with their complaints about their employer's behaviour.

Even though, in *Italy*, regulations and principles as formulated in the Decalogue 2004 play a large role in the protection of employees against privacy intrusion by CCTV, case law has played an important role in interpreting these regulations and determining the scope of application of Article 4 of the Workers' Statute. The result of the court decisions was that the use of CCTV in the workplace was severely restricted. In the decision in *Banco di Sicilia* v. *Fiba*,[36] the principal argument of the Court of Cassation [Supreme Court], was that the employees' right not to be monitored is considered a personal right, also stating that Article 4 is still applicable even if the employees are aware of the installation of CCTV. In other cases, the courts have also made it clear how the provisions of Article 4 Workers' Statute concerning the informing of employees on the installation of CCTV should be applied.

Article 4 also protects employees from camera surveillance that is aimed at improving or checking their performance at work. Furthermore, evidence that is obtained by CCTV is subject to Article 41 of the Constitution and also to Article 4 Workers' Statute. If the gathering of this evidence is found to be contrary to one of those regulations, it cannot be used in a court procedure.[37]

The lack of specific workplace privacy legislation has had its impact on the privacy protection of employees. In most countries, there seem to be no 'hard' standards that protect employees' workplace privacy interests. Instead, courts resort to balancing the interests of the employers and the employees. The case law demonstrates that this can be threatening to workplace privacy. In the United States, the reasonable expectation of privacy concept is also used in workplace privacy litigation and has had a negative effect on workplace privacy, since courts have held that the reasonableness of privacy expectations of employees in the workplace are low. Another important factor in the United States is the concept of 'at-will' employment, which puts the employees in a very vulnerable position.

This problem can be observed in more countries, where either the economically vulnerable position of employees or the fact that the outcome of legal procedures is very uncertain gives employers the upper hand in workplace privacy issues. Data protection commissioners have a positive influence on the workplace privacy situation of employees, but procedures are unfortunately in some cases based on complaints. In other countries, such as Belgium, the work of the data protection commissioner is not widely accepted or used by the courts.

The overall picture is that the lack of legislation has a negative effect on the privacy expectations of employees and that little has been done in general to strengthen their vulnerable position.

---

[36] *Banco di Sicilia* v. *Fiba*, Court of Cassation Decision 16 September 1997 No. 9211, PN 2004-184.

[37] *Società la Carica Veronesi Carla e C. S.A.S.* v. *Ledda*, Court of Cassation Decision of 17 June 2000, No. 82500, PN 2004-187.

### 13.3.3 **Future challenges**

As Phillips already noted, reasonable expectations of privacy may gradually diminish as a result of social developments. Once employees' consent to the employers' search and monitoring policies becomes customary, it will become part of the standard business activities and reduce employees' reasonable expectations of workplace privacy. When new technologies make searching, monitoring, and surveillance in general easier as well as cheaper, it is to be expected that an ever increasing number of employers will use surveillance technologies more actively and intensively in the near future. The present general legal framework on data protection combined with relevant provisions under the labour law framework (or, to put it differently, the absence of specific legal provisions in the area of workplace privacy) appears to be unable to prevent this from happening.

The European Commission is presently working on expanding the legal framework in the area of personal data protection. In addition to the general Data Protection Directive (95/46/EC), a data protection directive on privacy and electronic communications was issued several years ago: Directive 2002/58/EC.[38] Moreover, the European Commission has organised hearings to discuss a new plan for the protection of employees' data[39] which could lead to a specific data protection directive for the employment context. One of the topics in this new plan is the regulation of the consent of employees for the processing of personal data in an employer-employee relationship. In the employment context, consent can only be used in a limited way, caused by the fact that consent must be given freely and the employee must be able to withdraw his consent. This is often not the case in an employment relationship.[40]

Several of this book's contributors touched upon the topic of monitoring Internet and e-mail activities. It is a development that is clearly also on the agenda of the European Commission. In its working document, the Article 29 Data Protection Working Party offered guidance and concrete examples about what constitutes legitimate monitoring activities and the acceptable limits of workers' surveillance by the employer. [41]

---

[38] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31/07/2002 pp. 0037-0047.

[39] See *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data* (DG Employment and Social Affairs). On the Internet <http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf>. Last visited: July 2004.

[40] See Art. 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*. Adopted on 13 September 2001. WP 48, p. 23. On the Internet <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf>. Last visited: July 2004.

[41] See, for example, Art. 29 Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace*. Adopted on 29 May 2002. WP 55. On the

Among other topics, the European Commission plans to address the processing of employees' medical data, including drug tests and genetic tests, in a separate data protection directive.

According to the second stage consultation, there is a clear trend towards clarification of the general data protection principles to enable their application in the employment context. The open formulated general data protection principles and different interpretations in the employment context lead to unforeseen results, unclarity, and discrepancies between the letter of the law and the practice in the workplace. Therefore, several reasons exist for developing a specific legal framework for data protection in the employment sector: legal clarity and certainty, ensuring a more consistent and homogeneous application of the rules, the specificity of the employment context, and recent technological advances and their applications in the workplace.

The workers' privacy protection directive may improve working conditions. The Commission expects that a clarification of the rules will lead to better regulation, because it raises awareness of rights and obligations and is good for effective compliance.

The workers' privacy protection directive is also important in view of the integration of the European economy and the globalisation of the worldwide economy. As a result, a growing number of employees are working for companies with establishments or subsidiaries in multiple countries.

Workers' privacy protection is also part of the European Charter of Fundamental Rights. It can be found in Articles 1, 7, 8, 21, paragraph 1, and 31, paragraph 1.

These arguments for a workers' privacy protection directive seem also to be applicable to a reasonable expectation of privacy in the workplace. At least as far as data protection is concerned, a workers' privacy protection directive could result in more clarity on how much privacy and protection of workers' personal data can be expected.

## 13.4 General conclusions

### 13.4.1 **Reasonable expectations of privacy?**

Citizens' expectations of privacy have been reduced all over the world since the 11 September 2001 terrorist attacks in the US, given the new and extended powers for search and seizure which many investigative bodies have since received. We will not discuss the necessity of these measures, but we will focus on the question of what level of privacy people may expect, what the role of the different legal concepts is, and how this is reflected in the relevant case law. What do the current

---

Internet <http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_en.pdf>. Last visited: July 2004.

legislation, (self-)regulation, and case law mean in relation to privacy and data protection in the daily lives of citizens today? What will they mean in a future context with new technologies that may have the ability to collect more information, that are more affordable, and that may be less recognisable or unknown to the general public? Will they provide sufficient guidance to organisations that wish to employ camera surveillance, or employers that feel the need to monitor their employees? Although this study is limited to camera surveillance and workplace privacy, we will try to draw some general conclusions.

### 13.4.2 **Different contexts and content**

Although the countries surveyed have rather divergent legal regimes, a common ground is that, in most countries, the concept of a reasonable expectation of privacy is used in the case law in one way or another. In the United States, the concept's use is limited to search and seizure cases.

Both the concept and the context in which it is used differ between the various countries. Two variants of the reasonable expectation concept can be distinguished. The approach to the reasonable expectation concept in Europe and the US is of a subjective nature. The actual perception of the individual involved is relevant. Criminals have a lesser expectation because they can expect that the police may observe their (private) affairs as a consequence of their criminal activity. Something similar is happening in the workplace. It is justifiable that if a probable cause exists that an employee is involved in an illegal or harmful activity, that person's privacy may be invaded to a greater extent than would have been allowed normally. A person involved in such activities may expect such intrusions.

However, in Canada, a rather different approach is taken. The expectation is constructed upon the standards of privacy that people might expect in a 'free and democratic society'. There is no focus on the specific person challenging the legality of the search or seizure. Whether a person is involved in a criminal activity, for instance, is not relevant. This has a significant implication for the level of privacy to be expected. The Canadian approach is consistent with the opinion of the American Justice John Marshall Harlan in *United States* v. *White*. In a dissenting opinion, he said that: ''Criminals must not daily run the risks of unknown eavesdroppers prying into their private affairs; it subjects each and every law-abiding member of society to that risk'.[42]

This touches upon an important issue. From the case law in the areas of both workplace privacy and camera surveillance, we conclude that, in general, only those invasions of privacy are challenged in which the information obtained is used in criminal cases and dismissal cases. In these cases, the privacy intrusion is suffi-

[42] Dissenting opinion of Justice Harlan in *United States* v. *White*, 401 U.S. 745 (1971), p. 749. <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=401&invol=745>, PN 2004-201.

ciently important to go to court, because a person's freedom or significant monetary interests are at stake. A consequence of the reasonable expectation of privacy concept used in the United States and Europe is that the reasonable privacy expectations of 'criminals and other wrongdoers' are lower. People who engage in a criminal or wrongful activity may expect that their privacy will be invaded. Therefore, the case law does not draw a clear picture of what 'normal people' might expect. This is especially the case with camera surveillance technology that is permanently used to monitor behaviour in public areas and permanent workplace monitoring, for instance, of e-mail. The boundaries of what is allowed for normal people are not often discussed in case law. There is a danger that the boundaries found in case law that focus on 'criminals' and other 'wrongdoers' would also be used as a standard for 'normal people'. Fortunately, we found that other instruments such as self-regulating initiatives, codes of conduct and guidelines, and recommendations and opinions issued by data protection authorities to some extent fill in the reasonable expectation of privacy for citizens in general.

### 13.4.3 **The reasonable expectation of privacy v. the right to privacy**

According to Gellman, the importance of the legal privacy standard called 'reasonable expectation of privacy' will grow in the future, at least in the US. The importance of the reasonable expectation of privacy standard is stressed by the Fourth Amendment and by tort law, which protects people and not public or private places. The privacy standard offers a more general and flexible way to assess whether an individual's privacy has been invaded.

On the other hand, in relation to workplace privacy in the US, Phillips concluded that expectations of privacy in the workplace could diminish rather easily, for example, when employees' consent to employers' search policies becomes a standard business practice. According to Peter Blok in his comparative study,[43] since the 1970s, the concept of a *reasonable* expectation of privacy has evolved into *legitimate* expectation of privacy, due to the American Supreme Court. When there is no interference with the persons, houses, papers, and effects, mentioned in the Fourth Amendment, the Court is of the opinion that a citizen does not have a legitimate expectation of his privacy. This makes it much easier to reject an appeal that invokes privacy issues.

Article 8 ECHR also protects people rather than places: '*Everyone* (our emphasis) has the right to respect for his private and family life, his home and his correspondence'. A right to privacy seems stronger than the concept of a reasonable expectation of privacy. The Canadian Privacy Commissioner, George Radwanski, also

[43] Peter Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht* (Den Haag, Boom Juridische Uitgevers 2002), pp. 162-163.

addressed this issue (see Bennett and Bayley, Chapter 4). It seems to us that it may be easier to assess whether the right to privacy has been infringed upon than whether or not a reasonable expectation of privacy has been violated. However, when there is an interference with the right to privacy, the second question is whether the interference was in accordance with the law *and* necessary in a democratic society. From the ECHR case law, we may conclude in general that there may be an interference with the right to privacy, but, at the same time, the interference may be a legitimate one.

In the case of *P.G. and J.H.* v. *the United Kingdom*,[44] the Court concluded that a reasonable expectation of privacy is only one criterion to determine whether an interference with the right to privacy exists. The Court seems aware of the risk that applying this privacy standard may have. The use of the privacy standard might, at least in Europe, give rise to a lower level of privacy. From the fact that there is no reasonable expectation of privacy, the Court might conclude that there is no interference with the right to privacy (Article 8, paragraph 1 ECHR), and it might not refer to the accordance with the law and the necessity in a democratic society. This could lead to situations where governments would no longer need to have a legal basis or a necessity to interfere with the right to privacy.

In its recommendations on legislative proposals, the Dutch Data Protection Authority regularly points at the 'pressing social need' that, according to regular case law from the European Court of Human Rights, should legitimate any interference with the right to private life in Article 8 ECHR.[45] This means that an interference with the right to privacy is only legitimate when the interference is in accordance with the principles of proportionality and subsidiarity. An illustrative example is a recent statement by the Dutch Cabinet, that the extension of the Dutch identification requirement is necessary in a society that is becoming increasingly complex. The Cabinet added that extending the identification requirement is a relatively light measure, which is not disproportionate to the purposes to be achieved.[46]

Proportionality and subsidiarity seem to be principles that are very context-specific and time-dependent. Just like the reasonable expectation of privacy concept, the content of these principles seems to differ with the social and political developments. This raises the question of what concept or principle that does not depend on the interpretation of specific interests is the most useful. The two main concepts are the reasonable expectation of privacy concept and the concept of Article 8, paragraph 1, ECHR.[47] The latter seems stronger to us, because it clearly recognises the mere existence of privacy expectations in a free and democratic society. It is up to

[44] PN 2004-199.

[45] See, for example, College bescherming persoonsgegevens, Advies Wetsvoorstel uitbreiding identificatieplicht [Recommendation on the Extension of the Compulsory Identification Bill], 12 February 2003, z2002-1486.

[46] Kamerstukken II, 2003/04, 29 218, No. 3.

[47] This was also presented by Paul De Hert at the Privacy Colloquium in Tilburg on 21 April 2004.

the national authorities to prove that legislative measures that interfere with the citizens' private life can be based on a pressing social need. The European Court of Human Rights is the authority that should firmly and clearly approve or reject arguments for interference. Article 8 ECHR is also stronger from the citizens' perspective, because the authorities have to substantiate that the interference is legitimate. The reasonable expectation of privacy concept would be more unfavourable for the citizen, because he would have to prove the fact that he has a reasonable expectation of privacy in the first place, and why. It would also be more difficult to prove the existence of a reasonable expectation of privacy when it is related to the use of technologies that are accepted by a majority in society.[48]

As we noted in section 13.2.1.3, the English Court of Appeal has recently narrowed the wide interpretation of 'personal data' in the *Durant* case. As a result, the British Data Protection Act is no longer applicable to basic CCTV systems. The applicability of the Data Protection Act is determined not so much by the fact that personal data are being processed – or not – but by the intentions and goals of the CCTV controller. To us it seems that this judgment diverges from interpretations about the applicability of data protection legislation at the European level.

The Council of Europe has clearly stated that voices and images are protected as personal data under Convention No. 108 if they provide information about directly or indirectly identifiable individuals. The right to private life and the right to free movement are fundamental rights that are protected by Convention No. 108 and the European Convention for the Protection of Human Rights and Fundamental Freedoms. This has been confirmed several times by the European Court of Human Rights.

The Article 29 Data Protection Working Group concluded in their 2004 report (WP 89) that sound and image data are protected under EU Directive 95/46/EC if they provide information about directly or indirectly identifiable individuals.

In several EU countries, additional regulations and guidelines have been formulated: the UK Guidance, the Dutch Handreiking Cameratoezicht, and the Italian Decalogue. From all these legal documents, the European citizen can reasonably expect that his privacy will be respected in relation to CCTV.

Specific workplace privacy laws are rare, in the US as well as in Europe. It seems that only Finland has a specific statute on the protection of workers' privacy. Within Europe, the right to privacy in the workplace is recognised in several judgments by the European Court of Human Rights. In the EU, the general Data Protection Directive is applicable to the processing of workers' personal data. Interesting is the initiative of the European Commission to investigate the need for a separate directive to protect employees' personal data. Several developments, i.e., technological and socio-economic developments such as the integration of the European economies and the globalisation of the world economy, have led to the idea that clear

[48] See also the contribution by Robert Gellman in this book.

provisions for the protection of workers' personal data have become more important. Specific data protection issues for the employment context are the worker's consent for the processing of his personal data, access and processing of medical data in the employment context, drug testing and genetic testing in the employment context, and monitoring and surveillance in the workplace. Clarification of the data protection rights and obligations for employees and employers through a separate data protection directive might lead to a clearer view of the reasonable expectations of privacy for employees.

### 13.4.4 **Conclusion**

The country reports do not clearly show whether the legal concept of a reasonable expectation of privacy is a useful concept. Gellman thinks it is 'likely that the reasonable expectation test may be used more in the future (…)'. On the other hand, we have also seen the opinion that the concept of a reasonable expectation of privacy, at least in Canada and Europe, seems a weaker kind of protection than the fundamental right to respect for privacy, for example, as formulated in the European Convention on Human Rights. From *P.G. and J.H.* v. *United Kingdom*, it can be concluded that the European Court of Human Rights has become aware that using the concept of a reasonable expectation of privacy could result in less privacy protection. We agree with De Hert that lawyers can play an important role in the protection of privacy in criminal cases before the court, by paying more attention to data protection issues.[49] Although a court may deny the existence of a reasonable expectation of privacy, this does not mean that the data protection legislation is not applicable in cases concerning camera surveillance or workplace privacy. Therefore, the lawyer can force the court to test whether the processing of personal data, as a result of camera surveillance or workplace monitoring, is in accordance with data protection principles.

We are concerned that the concept of a reasonable expectation of privacy may easily be eroded as a result of social, political, and technological developments. Measures to combat terrorism, to fight against crime, and to increase security, together with the growing social acceptance of privacy-invasive technologies are the starting points for this privacy erosion. These developments emphasise the importance of a fundamental debate about the value of the reasonable expectation of privacy concept and about the future of this concept inside and outside Europe.

We fear that the reasonable expectation of privacy concept will become an easy legitimisation for interfering with a person's privacy, while it should lead to more fundamental questions. After all, should the reasonable expectation of privacy concept not be a kind of metaphor, to make politicians, citizens, organisations, compa-

[49] P.J.H. De Hert, F.P. Ölçer, 'Het onschadelijk gemaakte Europese privacybegrip. Implicaties voor de Nederlandse strafrechtspleging', *Strafblad. Het nieuwe tijdschrift voor strafrecht,* 2004/2, pp. 115-134.

nies, and other stakeholders aware of the fact that an important value in our free and democratic societies, the right to privacy, is being threatened by camera surveillance and workplace monitoring?